Dr. Zámbó Gyula*:
Pénzmosás határok nélkül

A jövedelemtermelő bűncselekmények, különösen az ember-, fegyver- és kábítószerkereskedelem szinte állandó kísérője a szintén bűncselekménynek minősülő pénzmosás. A bűnözők igyekeznek elfedni az illegális tevékenységekből származó pénz eredetét. Ennek egyik alapvető módszere a vagyon „utaztatása", azaz a bűncselekménnyel szerzett pénz országhatárokon keresztül történő mozgatása.

A legrégebbi, de napjainkban is gyakran használt módszer, hogy a bűncselekményből származó készpénzt kisebb címletekben, de nagy mennyiségben fizikailag szállítják más országokba, ahol abból különböző vagyontárgyakat (ékszert, gépjárművet, ingatlant) vesznek, vagy az adott ország pénzügyi-gazdasági rendszerébe juttatják bankokon, befektetési vállalkozásokon keresztül, esetleg cégek alapításával. Ehhez jellemzően olyan országokat keresnek, melyek bűnüldöző és igazságügyi rendszere sérülékenyebb, ahol a pénzmosás-megelőzési képességek gyengébbek.

A kereskedelemben és a pénzügyekben is egyre általánosabb digitalizáció, illetve a globalizált pénzügyi rendszerek, amelyek a készpénz táskákban történő szállításánál sokkal hatékonyabb pénzmosási megoldásokat is magukkal hoztak. Ma már pár kattintással a legkülönbözőbb ügyleteket hajthatjuk végre pillanatok alatt a világ szinte bármely pontján. Csak pár másodperc egy „láncátutalás" lebonyolítása, melynek során akár több ország különböző bankjainál vezetett számlákon fut át a tisztára mosandó pénz, hogy aztán egy távoli kontinensen működő cég webshopjában elköltsék azt. A nyomozó hatóságoknak azonban az országhatárok továbbra is akadályt jelentenek, így mire nemzetközi bűnügyi együttműködésben felgöngyölítenek egy ilyen tranzakciót, a bűnözők már rég kereket oldottak. Már ha egyáltalán sikerül a nyomozóknak az ügyletsorozat végéig eljutni. Ha a láncba egy kevésbé együttműködő országot is beillesztenek, gyakran fel sem tárható a pénz útja.

A digitalizáció kapcsán mindenképp szót kell ejteni a kripto eszközökről is. A kriptovaluták esetében – ahogy az az új technológiáknál, termékeknél gyakori – még nem alakultak ki hatékony ellenőrzési és felügyeleti rendszerek, a szektor szolgáltatói (kripto tőzsdék, pénztárca szolgáltatók stb.) még szintén gyakorlatlanok, kevésbé tudatosak a pénzmosás megelőzésben. A kriptovaluták azonban „országfüggetlenek", és már meg is jelentek az olyan kripto szolgáltatások (az ún. mixerek), amik lényegében teljesen követhetetlenné teszik ezen eszközök mozgatását, átruházását. Ráadásul a kriptovaluták a kezdetekben szorosan kapcsolódtak a darkweb illegális világához.

Mindez azonban nem csak a bűnözők és a bűnüldöző hatóságok ügye. Az utóbbi időkben rendkívüli módon megszaporodó számlacsalások kapcsán saját magunk is szembesülhetünk a „határok nélküliség" problémájával.

A számlacsalásoknak két fő módszere van. Az első a hagyományos csalások metódusát követi: a sértettet egy rendkívül kecsegtető ajánlattal, üzleti lehetőséggel veszik rá pénz átutalására. A másik módszer, hogy adathalászattal, kártékony szoftverek telepítésével, vagy éppen banki alkalmazottnak kiadva magukat szerzik meg a sértett netbanki hozzáféréshez szükséges kódját, jelszavát, aminek birtokában már maguk a csalók indíthatnak tranzakciókat, gyakran teljesen kiürítve az áldozat bankszámláját.

A csalárd utalások természetesen nem közvetlenül az elkövetőkhöz érkeznek. Ehhez rendszerint alvó cégek vagy pár tízezer forint ellenében közreműködő stróman személyek számláját használják. Nem ritka, hogy már ezen a ponton más országba vezetnek a szálak. A tapasztalatok azt mutatják, hogy az elkövetők még arra is figyelnek, hogy kipuhatolják a banki szűrőrendszerekben használt értékhatárokat, és azokat még éppen el nem érő tételekre bontva mozgassák a pénzt, ezzel is nehezítve a csalárd ügyletek észlelését.

A csaláshoz használt számlára rendszerint rövid idő alatt több sértettől érkeznek jóváírások, majd az így megszerzett pénzt elkezdik „utaztatni". További országokon átívelő tranzakciókat indítanak, hogy a leginkább szem előtt levő számláról mielőbb eltűntessék a csalással megszerzett pénzt, egyúttal elfedjék annak eredetét, nyomonkövetését ellehetetlenítsék.

Tanulságos példája a fentieknek az az eset, amikor egy olasz sértett abban a hiszemben utalt többezer eurót egy kelet-magyarországi bankfiókban vezetett számlára, hogy ő egy britt brókercégen keresztül Tesla részvényeket vásárolt. Ehelyett a magyar számláról szlovák, bolgár, török és kínai számlákra továbbították a pénzét, illetve részben kriptovalutát vettek belőle. S mire a hatóságoknak tudomására jutott az eset, addigra a magyar számlát nyitó cég már meg is szűnt.

Nyilvánvaló, hogy ilyen helyzetben szinte semmi esély nem marad a kicsalt pénz visszaszerzésére, gyakran még az elkövetők személyét sem sikerül megállapítani, hiszen csak emailben, esetleg telefonon léptek az áldozattal kapcsolatba.

Természetesen a bankok, a nyomozó hatóságok és pénzügyi felügyeleti hatóságként az MNB is igyekszik minimalizálni a károkat, azonban a legfontosabb a megelőzés, amihez az ügyfelek tudatossága elengedhetetlen. Ennek jegyében indította útjára 2022-ben az MNB a Bankszövetséggel, az Országos Rendőrfőkapitánysággal, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel és a Nemzeti Média- és Hírközlési Hatósággal a KiberPajzs programot, amelynek jelenleg már tizenegy együttműködő partnere van. A KiberPajzs honlapján számos hasznos információ és tanács található, hogy hogyan ismerhetők fel, hogyan kerülhetők el a csalók támadásai, és mik a teendők, ha ez mégsem sikerül.

A legfontosabb, hogy tájékozódjunk és mindig legyünk körültekintők! Ha mégis megtörténik a baj, egy percet szem szabad késlekedni, haladéktalanul jelezzük bankunknak és a rendőrségnek az esetet!

**A szerző a Magyar Nemzeti Bank Pénzmosás ellenőrzési osztályának felügyeleti csoportvezetője*

„Szerkesztett formában megjelent 2024. november 6-án a VG.hu oldalon."